Link Failure Detection in Computer Networks

Maximilian Brügge, Manuel Simon*
*Chair of Network Architectures and Services
School of Computation, Information and Technology, Technical University of Munich, Germany
Email: maximilian.bruegge@tum.de, simonm@net.in.tum.de

***Abstract*—In computer networks, data must be distributed over long distances, making it susceptible to errors. For this reason, there are specifically designed mechanisms in place to facilitate error recovery. This paper presents different mechanisms of failure detection in networks and classifies the approaches with respect to different failures types. Additionally, it discusses recovery mechanisms and how they correlate with these failure types, providing a holistic view of network resilience. This work underscores the importance of both detecting and effectively recovering from network failures to ensure uninterrupted operation and reliability.**

***Index Terms*—failure detection, fault detection, computer networks, mobile networks, wireless networks**

1. Introduction

As the digital landscape continues to evolve, networks have become the backbone of modern communication. These networks are not only made for data exchange but are also important to the functioning of applications across various domains. With their expansion and increased complexity, networks are now more susceptible to various failure types, ranging from minor transport errors, e.g. packet loss, to major disruptions [1]. This vulnerability highlights the importance of robust failure detection and recovery mechanisms. The ability to immediately and accurately identify failures is crucial in maintaining the reliability and efficiency of network systems. The types of failures encountered in these networks are varied, including hardware malfunctions, software bugs, and issues arising from network topology or design.

The focus of this paper is on selected failure detection in computer networks which are also considered reactive approaches. As outlined by Musumeci et al. [2] and Wang et al. [3], *reactive* strategies differ from *proactive* methods that are aimed at prevention. While *proactive* measures aim to prevent service disruptions, *reactive* approaches such as failure detection are imperative for initiating immediate recovery procedures. These procedures, crucial for swiftly repairing or replacing failed components and thus minimizing downtime, play a vital role in ensuring network resilience. This paper explores the methods and strategies employed for detecting failures in networks, categorizing these based on the types of network failures and presents appropriate recovery solutions. We investigate state-of-the-art and evolution of network reliability, underlining the challenges and advancements in this essential field of network management. This exploration contributes to enhancing the understanding and capabilities of network management, establishing the foundation for the successful deployment and operation of future-oriented networks. Specifically, it addresses the critical need for a very high probability of successful transmission, a key objective in 5G and 6G networks [4], ensuring their advanced performance and service continuity.

2. Technical Background

This section primarily focuses on the fundamental hardware components and essential software elements required for constructing a computer network. Additionally, we present various types of failures that can occur within a computer network.

2.1. Nodes

Peterson et al. [5] define a node as any device that connects to the network, like a computer or a router. These devices serve various roles, from running applications to directing data traffic. Any device capable of transmitting or receiving data to or from a network is classified as a node. In the Internet of Things (IoT), a dishwasher, for instance, could also represent a node within a network. Each node in a network has a limited amount of memory and processing capability, which is essential for processing data and throughput. These nodes are connected to the network via an adapter, which is operated through specialized software. The interplay between a node's memory capacity and its processing speed is a key factor in determining the overall efficiency of the network.

2.2. Links

Links are the channels that connect nodes, using mediums like cables or wireless space to transmit data. These media channels carry data in the form of electromagnetic signals across different frequencies. The physical nature of these links, whether they are made of fiber optics or copper wires, plays a significant role in how data is transmitted and at what speed. The design of these links, including their capacity to handle data and the method of encoding information, is fundamental to network functionality [5].

2.3. Cable-Related Failures

Cable-related failures are a special case of link failures which typically involve optical and copper fiber (i.e. Ethernet), respectively. Optical fiber breaks frequently occur

 doi: 10.2313/NET-2024-04-1_09

unintentionally at construction sites [1], [6]. Although these incidents may occasionally be observed by on-site workers, there are instances where such events go unnoticed by anyone [6]. For these cases, a sophisticated and reliable solution is needed. Another failure type related to optical fiber is high loss, which can occur during installation when workers make errors. These may involve improper fiber bending, contamination of connectors, mishandling of tools, or incorrect connections as described by Fernández et al. [7].

2.4. Wireless Network Failures

Wireless networks present a unique set of failure scenarios, distinct from cable-based networks. These failures are primarily influenced by environmental and physical aspects of wireless signal transmission and reception. Interference is a major cause of wireless network failure. External sources like other electronic devices or physical obstructions can disrupt signal transmission, leading to signal degradation or loss as discussed by M. Gast [8]. Additionally, atmospheric conditions such as heavy rain or fog can also impact signal strength as shown by Osahenvemwen and Omatahunde [9]. Moreover, hardware failures in wireless network components such as routers, access points, and base stations can lead to network outages. Unlike wired networks, where issues might be localized to specific cable faults, failures in key wireless components can have a widespread impact, affecting a large number of users.

Network overload is another critical challenge across all network types, impacting both wireless and wired systems. High device density or excessive data traffic can lead to congestion in any network, potentially causing service outages or significant performance reduction. This phenomenon is especially relevant in wireless networks due to inherent constraints such as limited spectrum and susceptibility to interference as described by C. Casetti et al. [10]. They also describe how the network can become congested, leading to service outages or severe performance degradation. This is particularly evident in both mobile and residential wireless networking environments, where the increasing demand for high-bandwidth applications strains the network's capacity.

3. Failure Detection Mechanisms

This section explores mechanisms employed for detecting failures in computer networks. The complexity and critical nature of networks necessitate robust and precise methods to swiftly identify and address issues, ensuring network reliability and efficiency. We delve into several key technologies and methodologies that have been developed to detect, analyze, and localize failures.

3.1. Optical Time-Domain Reflectometry

When a fiber break occurs, it can be noticed that no packets are received by the recipient anymore, while at the same time the node is also not reachable. This raises the question of whether the issue is link or node-related. For monitoring optical fiber, we can use an Optical Time-Domain Reflectometer (OTDR), which is a leading technique for monitoring optical networks and was developed in 1976 by Barnoski and Jensens [11]. They describe how OTDR operates using Rayleigh scattering, where light reflects off particles smaller than its wavelength. Using this method, a pulsed laser sends light into an optical fiber, creating backscattered light that is detected by a photodiode. This involves sending multiple light pulses during a set measurement time and averaging the traces to enhance accuracy and resolution. The choice of pulse width and measurement times involves trade-offs: shorter pulse widths provide higher resolution but may increase noise and reduce signal visibility due to lower emitted power [11]. In telecom networks, technicians often balance these factors, selecting pulse widths that optimize both resolution and signal clarity. After running a trace generation, OTDR devices yield time-series data which can be automatically analyzed or plotted. High peaks or huge losses in the data usually indicate an error at that position in the fiber. Figure 1 showcases an exemplary OTDR trace, highlighting the use of PC and APC connectors, a power splitter, and Optical Network Units (ONU). This trace vividly illustrates the backscattered light patterns generated by the pulsed laser, marked by significant peaks and troughs. These variations are critical for identifying faults along the fiber, demonstrating the OTDR's precision in fault localization.

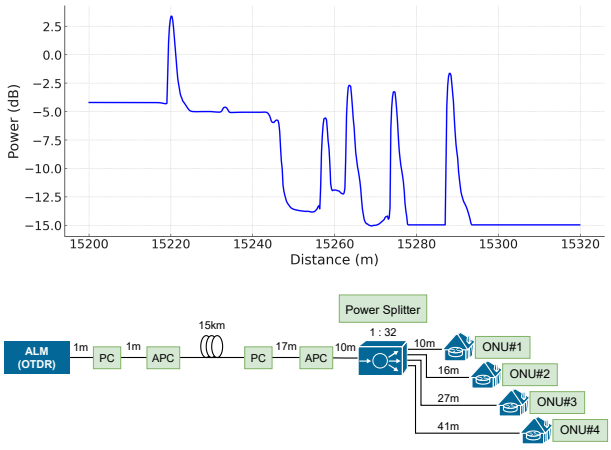

Figure 1: Exemplary OTDR trace using PC and APC Connectors, Power Splitter, and Optical Network Units (ONU)

Advantages of OTDR include its high accuracy and resolution, which allow for precise fault localization. It also enables non-invasive testing, as faults can be detected without physically accessing the entire length of the cable. Additionally, OTDR is versatile, suitable for various fiber types and lengths, and aids in predictive maintenance by detecting potential issues early on. However, there are some disadvantages to using OTDR. As can be seen in Figure 1, the complexity of OTDR traces requires skilled interpretation, especially in networks with intricate architectures. To counteract this, recent advancements have been made in interpreting this data. It has been shown that the characteristics of the different peaks in OTDR traces can be effectively classified using deep learning [12]. This approach significantly enhances the accuracy and

efficiency of fault detection and localization in optical networks.

3.2. Quality of Transmission

Quality of Transmission (QoT) is a metric in evaluating the performance and reliability of optical devices in computer networks. It encompasses the effects of factors such as device ageing and external environmental changes, such as temperature variations, which can progressively degrade transmission quality. Understanding and analyzing QoT is essential for detecting gradual impairments and implementing timely solutions to ensure sustained network efficiency and effectiveness. S. Barzegar et al. [13] discuss two of the most used QoT mechanisms which are discussed in this section.

Bit Error Rate (BER): BER is a measure of the number of bit errors in a transmitted signal. Vela et al. [14] classify BER as a critical metric for assessing the signal quality of optical connections. It becomes particularly relevant in scenarios where signal integrity is compromised due to various types of failures. E.g., signal overlap occurs when an optical connection's spectrum allocation interferes with a neighboring one, often due to inaccuracies in the central frequency of lasers or filters. Tight filtering is another issue, arising from misalignments or inaccuracies in the filter's central frequency or width. Gradual drift happens when the optical signal or filter slowly deviates from its initial central frequency, while cyclic drift is characterized by periodic deviations over time. These failures can lead to sudden or gradual increases in BER. Detecting and analyzing these variations in BER is crucial for identifying and addressing the underlying causes of signal degradation, ensuring the reliability and efficiency of optical network communications. In this context, advanced algorithms, i.e., BANDO and LUCIDA [14], are proposed to detect BER degradation and identify failure patterns, respectively, enhancing the monitoring and management of optical networks.

Signal-to-Noise Ratio (SNR): The level of a desired signal in relation to the background noise level is measured using the SNR. In the work of C. Alkemade et al. [15] the authors delve into the concept of SNR, which they define as the ratio of the power of a signal to the power of the noise and is usually expressed in decibels. A higher SNR indicates a clearer and less noisy signal, making it a crucial parameter in optimizing the performance of communication and detection systems. Figure 2 illustrates the concept of SNR, depicting how signal power compares to noise power in a visual format.

3.3. Received Signal Strength Indicator

Received Signal Strength Indicator (RSSI) is a critical tool used in the realm of wireless networking, particularly in identifying and managing the stability and performance of connections like Wi-Fi access points or mobile networks. According to Y. Chapre et al. [17], it serves as a valuable mechanism for failure detection. RSSI measures the power of signals received by a wireless device. In essence, RSSI measures the signal's strength at a specific location and time. The strength of the received signal is primarily determined by the distance between

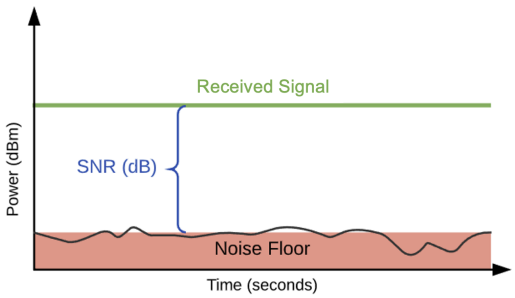

Figure 2: Signal-to-Noise Ratio [16]

the transmitter and the receiver. However, it is not just about distance; various factors can influence RSSI values, making it a dynamic and sensitive measure. For instance, Wi-Fi networks operating in densely populated areas often experience decreased RSSI values due to interference from multiple nearby routers transmitting on the same or overlapping channels. In a typical IEEE 802.11b/g/n network [18], extensive measurements are taken to analyze these factors affecting RSSI. This analysis helps in understanding the reliability and performance of the network under various conditions. The effectiveness of RSSI as a failure detection mechanism lies in its ability to provide a real-time snapshot of the network's signal strength. By continuously monitoring RSSI values, network administrators can quickly identify and address areas with weak signals, ensuring optimal network performance and reliability.

4. Recovery Mechanisms

It is not only crucial to identify network failures but also to address them, ensuring continued network operation. Following the presentation of link failure mechanisms in computer networks, this section shifts focus to recovery techniques and strategies. Rapid recovery is essential to maintain the network's reliability and efficiency. We will discuss various technologies and methods that support seamless network operations even after disruptions.

4.1. Lightpath Re-Routing

Lightpath re-routing in optical networks, particularly those utilizing dense wavelength division multiplexing (DWDM) and optical switches, is a process for ensuring efficient and reliable network operations, as explored by Bouillet et al. [19] in their research. These networks manage service requests through an online routing algorithm that dynamically decides the best routing paths based on current network information. The challenge lies in maintaining service continuity, especially given the high connection rates of these networks, which can reach tens of Terabits per second. Two restoration strategies are employed in these networks: end-to-end dedicated mesh protection and shared mesh restoration. The dedicated mesh approach uses predefined backup paths that are diverse from the primary paths, ensuring that both do not fail simultaneously. This method requires significant capacity, as backup paths are often longer than primary

TABLE 1: Overview of all discussed detection mechanisms

Detection Mechanism	Hardware Level	Failure Types	Recovery Mechanisms	Literature
Optical Time Domain Reflectometry (3.1)	Optical Fiber/Devices	Optical fiber bend, break, loss	Lightpath Re-Routing (4.1)	[11], [12], [19]
Quality of Transmission (3.2)	Link	Signal degradation, noise interference	Lightpath Re-Routing (4.1)	[13]–[15], [19]
Received Signal Strength Indicator (3.3)	Link	Interference, Distance, Obstructions, Malfunction	Dynamic Channel Assignment (4.2)	[17], [18], [20]

paths. However, it offers the advantage of immediate restoration due to the permanence of the backup paths. In contrast, shared mesh restoration allows backup paths to share capacity, provided the primary paths are mutually diverse. This approach saves more space in the network but is slower to recover, as it requires additional steps to establish a backup route. The length and number of hops of the backup path can influence the restoration time, posing a trade-off between cost and recovery latency.

4.2. Dynamic Channel Assignment

In Wireless Local Area Networks (WLANs), a channel refers to a specific frequency range in the radio spectrum for wireless communication. Figure 3 illustrates the 2.4GHz Wi-Fi channel band, highlighting the available channels within this spectrum. Strategically selecting Access Point (AP) channels is crucial for enhancing network performance, especially in dense environments where overlapping frequencies may cause interference. This overlap leads to interference and network congestion, adversely affecting network functionality. The impact of interference is closely monitored using the RSSI (c.f. Section 3.3). Advanced channel assignment algorithms aim to minimize the impact of interference. By focusing on reducing the interference impact, these algorithms can significantly improve data transmission quality and overall network reliability. The effectiveness of advanced algorithms, such as Wi-5, has been demonstrated through real-world evaluations. [20]

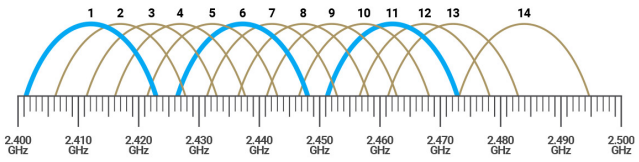

Figure 3: 2.4GHz Wi-Fi Channel Band [21] based on D. Coleman et al. [22]

5. Conclusion and Future Work

This paper has presented an overview of various link failure detection mechanisms in computer networks, emphasizing the significance and applicability of each method under different failure scenarios. The detailed analysis, as summarized in Table 1, provides a clear comparison of these mechanisms, highlighting the involved hardware, failure types and their possible recovery.

The advancements in technologies such as deep learning, as mentioned, offer promising avenues for enhancing the efficiency and accuracy of these detection methods. This paper has underscored the importance of selecting appropriate detection mechanisms based on the specific nature of the potential failures, a decision critical for maintaining the robustness and reliability of optical networks. Future research may focus on the integration of artificial intelligence and machine learning to further refine these detection methods, potentially automating the process and providing more nuanced insights into network health and integrity. The evolving landscape of optical network technology continues to present new challenges and opportunities, making ongoing research and development in this field necessary.

References

[1] Spiegel, "Bauarbeiten offenbar Ursache von IT-Ausfall bei der Lufthansa," Februrary 15, 2023, Accessed: February 29, 2024. [Online]. Available: https://www.spiegel.de/wirtschaft/unternehmen/lufthansa-bagger-kappt-kabel-bauarbeiten-offenbar-ursache-von-it-ausfall-a-bb48b9e6-3c5b-4f22-9726-75de334525bc

[2] F. Musumeci, C. Rottondi, G. Corani, S. Shahkarami, F. Cugini, and M. Tornatore, "A tutorial on machine learning for failure management in optical networks," *Journal of Lightwave Technology*, vol. 37, no. 16, pp. 4125–4139, 2019.

[3] D. Wang, C. Zhang, W. Chen, H. Yang, M. Zhang, and A. P. T. Lau, "A review of machine learning-based failure management in optical networks," *Science China Information Sciences*, vol. 65, no. 11, p. 211302, 2022.

[4] A. Gupta, X. Fernando, and O. Das, "Reliability and availability modeling techniques in 6g iot networks: A taxonomy and survey," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, 2021, pp. 586–591.

[5] L. L. Peterson and B. S. Davie, *Computer networks: a systems approach*. Elsevier, 2007.

[6] M. Illidge, "Construction causes major cable break in Johannesburg — and almost no-one knew," October 11, 2023, Accessed: February 29, 2024. [Online]. Available: https://mybroadband.co.za/news/fibre/510900-construction-causes-major-cable-break-in-johannesburg-and-almost-no-one-knew.html

[7] M. P. Fernández, L. A. B. Rossini, J. P. Pascual, and P. A. C. Caso, "Enhanced fault characterization by using a conventional otdr and dsp techniques," *Opt. Express*, vol. 26, no. 21, pp. 27 127–27 140, Oct 2018. [Online]. Available: https://opg.optica.org/oe/abstract.cfm?URI=oe-26-21-27127

[8] M. Gast, *802.11 wireless networks: the definitive guide*. " O'Reilly Media, Inc.", 2002.

[9] A. O. Osahenvemwen and B. E. Omatahunde, "Impacts of weather and environmental conditions on mobile communication signals," *Journal of Advances in Science and Engineering*, vol. 1, no. 1, pp. 33–38, Apr. 2018. [Online]. Available: http://www.sciengtexopen.org/index.php/jase/article/view/8

[10] C. Casetti, M. Gerla, S. Mascolo, M. Y. Sanadidi, and R. Wang, "TCP westwood: end-to-end congestion control for wired/wireless networks," *Wireless Networks*, vol. 8, pp. 467–479, 2002.

[11] M. K. Barnoski and S. M. Jensen, "Fiber waveguides: a novel technique for investigating attenuation characteristics," *Appl. Opt.*, vol. 15, no. 9, pp. 2112–2115, Sep 1976. [Online]. Available: https://opg.optica.org/ao/abstract.cfm?URI=ao-15-9-2112

[12] M. Brügge, J. Müller, S. K. Patri, S. Jansen, J. Zou, S. Althoff, and K.-T. Förster, "Live demonstration of ML-based PON characterization and monitoring," in *2023 Optical Fiber Communications Conference and Exhibition (OFC)*, 2023, pp. 1–3.

[13] S. Barzegar, M. Ruiz, A. Sgambelluri, F. Cugini, A. Napoli, and L. Velasco, "Soft-failure detection, localization, identification, and severity prediction by estimating QoT model input parameters," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 2627–2640, 2021.

[14] A. P. Vela, M. Ruiz, F. Fresi, N. Sambo, F. Cugini, G. Meloni, L. Potì, L. Velasco, and P. Castoldi, "BER degradation detection and failure identification in elastic optical networks," *Journal of Lightwave Technology*, vol. 35, no. 21, pp. 4595–4604, 2017.

[15] C. Alkemade, W. Snelleman, G. Boutilier, B. Pollard, J. Winefordner, T. Chester, and N. Omenetto, "A review and tutorial discussion of noise and signal-to-noise ratios in analytical spectrometry—i. fundamental principles of signal-to-noise ratios," *Spectrochimica Acta Part B: Atomic Spectroscopy*, vol. 33, no. 8, pp. 383–399, 1978. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0584854778800494

[16] Hollyland, "All about signal to noise ratio," https://www.hollyland.com/blog/tips/signal-to-noise-ratio, 10 2023, Accessed: February 29, 2024.

[17] Y. Chapre, P. Mohapatra, S. Jha, and A. Seneviratne, "Received signal strength indicator and its analysis in a typical wlan system (short paper)," in *38th Annual IEEE Conference on Local Computer Networks*, 2013, pp. 304–307.

[18] "IEEE standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac)and physical layer (phy) specifications amendment 5: Enhancements for higher throughput," *IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009)*, pp. 1–565, 2009.

[19] E. Bouillet, J.-F. Labourdette, R. Ramamurthy, and S. Chaudhuri, "Lightpath re-optimization in mesh optical networks," *IEEE/ACM Transactions on Networking*, vol. 13, no. 2, pp. 437–447, 2005.

[20] A. Raschellà, M. Mackay, F. Bouhafs, and B. I. Teigen, "Evaluation of channel assignment algorithms in a dense real world wlan," in *2019 4th International Conference on Computing, Communications and Security (ICCCS)*, 2019, pp. 1–5.

[21] EnGenius Technologies, Inc., "Your Go-To-Guide for Channel & Transmit Power on Wi-Fi Networks (Part 2)," https://www.engeniustech.com/wp-content/uploads/2017/10/blog_nov1.jpg, 10 2017, Accessed: February 29, 2024. [Online]. Available: https://www.engeniustech.com/go-guide-channel-transmit-power-wi-fi-networks-2/

[22] D. D. Coleman and D. A. Westcott, *Cwna: certified wireless network administrator official study guide: exam Pw0-105*. John Wiley & Sons, 2012.